CSE 291 / Math 277A - Quantum Complexity Theory	October 27, 2022
Lecture 10	
Lecturer: Daniel Grier	*Scribe: Philip Lamkin*

1 Warmup

Recall the collision problem from Lecture 8:

COLLISION:
Oracle: $f\colon \{0,1\}^n \to \{0,1\}^n$
Goal: Promised that f is 1-to-1 or 2-to-1, decide which

Fact 1. *Suppose f is 2-to-1. Then for randomly chosen $A, B \subseteq \{0,1\}^n$ with $|A||B| = 2^n$ there is a constant probability that $\exists a \in A, b \in B$ with $f(a) = f(b)$.*

Theorem 2 (Brassard, Høyer, and Tapp [BHT97])**.** *The quantum query complexity of* COLLISION *is $O(2^{n/3})$.*

Proof. Pick a random A of size $2^{n/3}$ and B (disjoint from A) of size $2^{2n/3}$. First query each element of A, which takes $2^{n/3}$ queries. With this, construct the (single query) function $g(x)$ which returns true if there is $a \in A$ with $f(x) = f(a)$. Now run Grover's algorithm on B, to see if g is ever true. This takes $O(\sqrt{2^{2n/3}}) = O(2^{n/3})$ queries.

If f is 2-to-1, then there is a constant probability this algorithm returns true. By iterating a sufficient constant number of times, we can get the probability to be at least $2/3$ that we find at least one success. If f is 1-to-1, g will always be the constant 0 function. Therefore we run Grover's algorithm a constant number of times, and return true if Grover's ever accepted, and otherwise returns false. This algorithm solves COLLISION with $O(2^{n/3})$ queries. □

2 BVVV lower bound for Grover

Recall where we left last time, with two states $|\phi\rangle$ and $|\psi\rangle$ such that $\||\phi\rangle - |\psi\rangle\|_2 \leq \frac{T}{\sqrt{2^n}}$, where T is the total number of queries we made, and $|\phi\rangle$ and $|\psi\rangle$ are the states corresponding to running our proposed algorithm on the all 0's string versus the string that has one (carefully chosen) 1.

In other words, if T is not sufficiently large, then the two potential states are extremely close to each other (in ℓ_2 distance). We want to show that if they are close together in ℓ_2 distance, then all measurement procedures fail to distinguish them with high probability. To formalize this, let us define the *total variation distance* between two discrete probability distributions p, q:

$$\mathrm{TV}(p,q) = \frac{1}{2}\|p - q\|_1 = \frac{1}{2}\sum_i |p_i - q_i|.$$

The total variation distance is important because it determines the maximum probability with which we can distinguish two probability distributions. That is, suppose with 50% probability we sample from p and with 50% probability we sample from q, the maximum probability with which we can guess which distribution was sampled from is $1/2 + \mathrm{TV}(p,q)/2$.

Lemma 3. *If $\||\phi\rangle - |\psi\rangle\|_2 < \epsilon$, then the total variation distance from measuring $|\phi\rangle$ and $|\psi\rangle$ is at most 2ϵ.*

Proof. Suppose $|\phi\rangle = \sum \alpha_x |x\rangle$, $|\psi\rangle = \sum \beta_x |x\rangle$. For ease of notation, assume α_x, β_x are all reals, though the proof still works if we allow them to be complex. Let $\gamma_x = \beta_x - \alpha_x$. Now we write

$$\||\phi\rangle - |\psi\rangle\|_2 = \sqrt{\sum_x \gamma_x^2} \leq \epsilon.$$

Let p, q be the distributions of measuring ϕ, ψ respectively. Then, we have that twice of their total variation distance is given by

$$\begin{aligned}
\sum_x |\alpha_x^2 - \beta_x^2| &= \sum_x (\beta_x - \alpha_x)(\beta_x + \alpha_x) \\
&= \sum_x \gamma_x(\gamma_x + 2\alpha_x) \\
&\leq \sum_x \gamma_x^2 + 2|\gamma_x \alpha_x| && \text{(triangle inequality)} \\
&\leq \|\gamma\|_2^2 + 2\|\gamma\|_2 \|\alpha\|_2 && \text{(Cauchy–Schwarz)} \\
&\leq \epsilon^2 + 2\epsilon\,,
\end{aligned}$$

which is at most 4ϵ since $\epsilon \leq 2$ by the triangle inequality ($\||\phi\rangle - |\psi\rangle\|_2 \leq \||\phi\rangle\|_2 + \||\psi\rangle\|_2 = 2$). Hence the TV distance is at most 2ϵ. □

Theorem 4. *Grover's algorithm is optimal. The quantum query complexity of* OR *is* $\Omega(2^{n/2})$.

Proof. We have just shown that for an algorithm with T queries, there is a state we should accept and one we should reject which we can distinguish with probability at most $\frac{1}{2} + \frac{T}{\sqrt{2^n}}$. To correctly answer at least $2/3$ of the time, this must be at least a constant larger than $1/2$, which requires $T = \Omega(2^{n/2})$. □

3 Polynomial Method for Grover Lower Bound

Now we introduce a powerful method for proving lower bounds, known as the polynomial method. For this purpose, it is convenient to consider the function $f\colon \{0,1\}^n \to \{0,1\}$ as a long bit string $x = x_1 x_2 \dots x_{2^n}$ where $x_i = f(\mathrm{Bin}(i))$. Here, $\mathrm{Bin}(i)$ means the binary representation of i. Let us also write $N := 2^n$.

In this language, the goal for the OR problem is to determine whether any x_i is equal to 1. Suppose we have a quantum query algorithm that solves this question. We start by applying a arbitrary followed by an oracle call:

$$|0\rangle \to \sum_{i=1}^N \alpha_i |i\rangle \to \sum_{i=1}^N (-1)^{x_i} \alpha_i |i\rangle\,.$$

Note that in general, we would also need to have an ancilla register, but the analysis is identical, so we have omitted it for clarity. The key observation is that $x_i \in \{0,1\}$ implies $(-1)^{x_i} = 1 - 2x_i$. Hence we can write this state as

$$\sum_{i=1}^N (1 - 2x_i)\alpha_i |i\rangle\,.$$

In other words, the amplitudes of our state after a single quantum query are polynomials in the variables $x_1, \dots, x_N$. In fact, we now claim by induction that after T queries, the amplitudes will be polynomials of degree T in $\{x_i\}$. This proof relies on the following ideas (i) applying a phase oracle increases the degree of the polynomial by 1 as we have seen above and (ii) applying any unitary does not increase the degree.

Now that we have that, suppose after making all T of our oracle calls and applying unitaries we end up in some state

$$|\psi\rangle = \sum_{i=1}^N \alpha_i(x) |i\rangle\,,$$

where each $\alpha_i(x)$ is a degree T polynomial in $x_1, x_2, \dots x_N$. Our acceptance probability is $\langle\psi| P |\psi\rangle$ for some projector P which is determined by the measurement outcomes we accept (e.g., measuring the first qubit corresponds to the projector $P = |0\rangle\langle 0| \otimes I$). Expanding out this probability

$$\left(\sum_{i=1}^N \alpha_i^*(x) \langle i|\right) P \left(\sum_{j=1}^N \alpha_j(x) |j\rangle\right) = \sum_{i,j=1}^N \alpha_i^*(x)\alpha_j(x) \langle i| P |j\rangle$$

we see that it is a which is a degree $2T$ polynomial. Let's call it $p(x)$.

We note that the problem we consider is symmetric: no matter what permutation we apply to the string x, the answer to "whether there exists a 1 in the string" should not change. Now, consider another polynomial q which is the sum of all results of p after applying an arbitrary permutation.

$$q(x) = \frac{1}{N!} \sum_{\pi \in S_N} p(\pi \cdot x)$$

where we denote by $\pi \cdot x$ as the result of applying the permutation to the bit string x, i.e. $\pi \cdot (x_1, x_2, \ldots x_n) = (x_{\pi(1)}, x_{\pi(2)}, \ldots x_{\pi(N)})$. By our previous observation (the problem's answer is invariant under permutation of the input string), $q(x)$ should also be at least the acceptance probability of the algorithm. Furthermore, $q(x)$ is now symmetric.

To be clear, $q(x)$ is a multivariate polynomial in $x_1, \ldots, x_N$. However, we now claim that because $q(x)$ is symmetric it can be written as a univariate polynomial of the same degree $r(z)$ where $z = \sum_{i=1}^{N} x_i$.

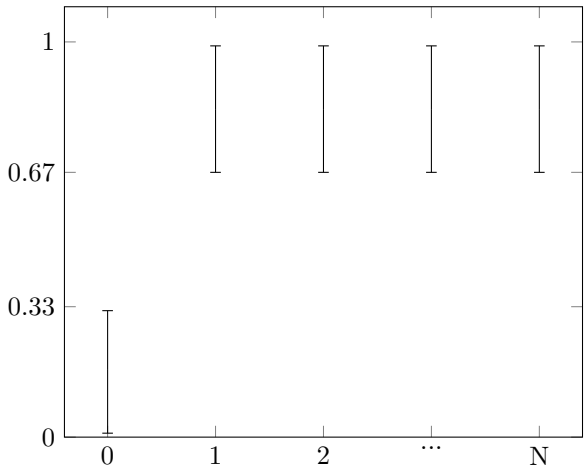
To show this, we will use the following fact: for every symmetric polynomial over Boolean variables, the coefficients of all terms of the same degree are equal. To prove this, simply take the smallest degree for which this is not true and consider the two terms with different coefficients. Setting the variables to be all 1's in one term and the rest 0's gives a different result from setting the variables to be all 1's in the other term and the rest 0's. Since both terms have the same number of variables, this is a contradiction because the function was supposed to be symmetric.

Let β_i be the coefficient of any term in $q(x)$ which has degree i. Notice that our new variable $z = \sum_{i=1}^{N} x_i$ counts the number of variables which are 1. Therefore, using the above argument, we can write

$$q(x) = \sum_{i=0}^{\deg q} \beta_i \binom{z}{i} = \sum_{i=0}^{\deg q} \beta_i \frac{z(z-1)\cdots(z-i+1)}{i!} = r(z)$$

as the expression that counts how many terms in the original expansion of $q(x)$ had the same degree.

Let's return to our specific problem. To summarize, we have a polynomial $r(z)$ of degree $2T$ which captures the acceptance probability of the quantum algorithm. If the quantum algorithm were perfect (i.e., had no error), then $r(0) = 0$ and $r(z) = 1$ for all $z \neq 0$. Since the quantum algorithm can err with probability at most $1/3$, the acceptance probabilities must have values in the following ranges:



To be clear, the polynomial $r(z)$ can do whatever it likes on non-integer points, but on the values $0, 1, \ldots, N$, it must fall within the specified ranges. We now want to show that any polynomial which has that behavior must necessarily have relatively high degree. Specifically, we can apply the Markov brothers' inequality:

Theorem 5 (Markov brothers' inequality)**.** *If $p(x)$ is a polynomial, then*

$$\max |p'(x)| \leq \left| \frac{\max p(x) - \min p(x)}{N} \right| (\deg p)^2,$$

where the max and min values are for $0 \leq x \leq N$ and $p'(x)$ denotes the first derivative.

Theorem 6. *If $r(z)$ as above has the desired properties, then $T = \Omega(\sqrt{N})$.*

Proof. Plugging in r to the Markov brothers' inequality and rearranging and weakening slightly gives us

$$N \max_{0 \le z \le N} |r'(z)| \le \max_{0 \le z \le N} r(z)(2T)^2$$

Let $M = \max_{0 \le z \le N} r(z)$, and pick z_0 with $r(z_0) = M$ (we can do so since $[0, N]$ is compact). Let's analyze two possible cases:

- $M < 2$: Note this is the "most likely" case, since we don't expect our function to go skyrocketing. In order to have $r(0) \le 1/3$ and $r(1) \ge 2/3$, by the mean value theorem there must be some $z \in [0, 1]$ with $r'(z) \ge 1/3$. Plugging this into the brothers' inequality, we get

  $$\frac{N}{12T^2} \le \frac{N}{4T^2} \max |r'(z)| \le \max r(z) < 2$$

  so in this case we know that $T = \Omega(\sqrt{N})$.

- $M \ge 2$: In this case, the mean value theorem implies that $|r'(c)| \ge 2(M-1)$ for some $c \in [\lfloor z_0 \rfloor, \lceil z_0 \rceil]$, since r must return down to at most 1 for each integer, and the closest integer is at most $1/2$ away. We get $2N(M-1) \le M(2T)^2$, so

  $$\frac{N}{2T^2} \le \frac{M}{M-1} \le 2$$

  and hence again we know that $T = \Omega(\sqrt{N})$.

□

Combining everything together, we get a new proof of Theorem 4 using the polynomial method:

Proof: (Theorem 4). Any quantum query algorithm that approximates OR with T queries gives rise to a polynomial r of degree $2T$ that approximates OR. By Theorem 6, any such polynomial must have degree $\Omega(\sqrt{N})$. Hence, $d = \Omega(\sqrt{N})$. □

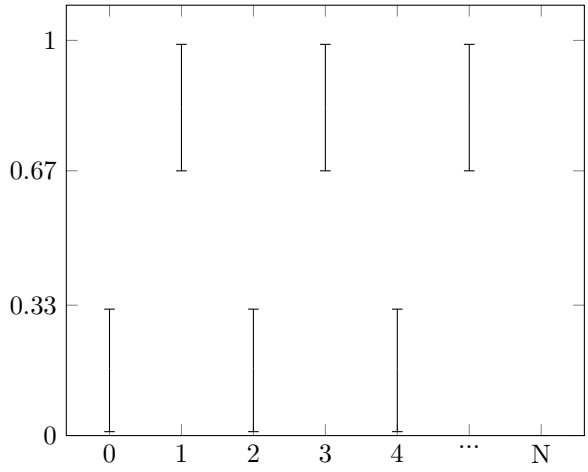
Remark 7. *If we want perfect accuracy, $r(z) = 1$ for $z = 1, 2, \ldots N$, so the fundamental theorem of algebra tells us that $\deg r \ge N$, so we need at least $N/2$ queries.*

4 Complexity of Parity

We've seen the Deutsch-Josza algorithm which can compute $x_1 \oplus x_2 \ldots \oplus x_N$ in $N/2$ quantum queries. We claim this is tight.

Theorem 8. *The quantum query complexity of the parity function is precisely $N/2$.*

Proof. The parity function is symmetric, so running the polynomial method as above again gives us $r(z)$ which must now have values in these ranges:



In particular, $r(z) = 1/2$ at N distinct values, one each between i and $i+1$ for $0 \leq i < N$. Thus by the fundamental theorem of algebra, $\deg r \geq N$. Since the degree of r is at most twice the number of queries, we must have made at least $N/2$ queries. □

5 Ambainis' Adversary Method

We now present the setup for one final method for proving that the query complexity of OR is $\Omega(\sqrt{N})$.

Theorem 9 (Ambainis' Adversary Method [Amb00])**.** *Suppose $f\colon \{0,1\}^N \to \{0,1\}$. Let $X, Y \subseteq \{0,1\}^N$ be such that $\forall x \in X, f(x) = 0$ and $\forall y \in Y, f(y) = 1$. Let $R \subseteq X \times Y$ be a relation such that*

1. *For every $x \in X$, there are at least m_0 inputs $y \in Y$ such that $(x,y) \in R$.*
2. *For every $y \in Y$, there are at least m_1 inputs $x \in X$ such that $(x,y) \in R$.*
3. *For every $x \in X$ and $i \in \{1,\ldots,N\}$, there are at most s_0 inputs $y \in Y$ with $(x,y) \in R$ and $x_i \neq y_i$.*
4. *For every $y \in Y$ and $i \in \{1,\ldots,N\}$, there are at most s_1 inputs $x \in X$ with $(x,y) \in R$ and $x_i \neq y_i$.*

Then the quantum query complexity of f is $\Omega\left(\sqrt{\frac{m_0 m_1}{s_0 s_1}}\right)$.

Now we apply this to OR. Let $X = \{0^N\}$, $Y = \{\text{all strings with exactly one 1}\}$, and $R = X \times Y$. Then $m_0 = N$, $m_1 = 1$, $s_0 = 1$, $s_1 = 1$, so the query complexity is $\Omega(\sqrt{N})$.

References

[Amb00] Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, pages 636–643, 2000.

[BHT97] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum algorithm for the collision problem. *arXiv quant-ph/9705002*, 1997.